REMARKS

Status of the Claims

Claims 1, 3-11, 13-21, and 23-30 are currently present in the Application, and claims 1, 11, and 21 are independent claims. Claims 1, 3, 11, 13, 21, 23, 24, and 26 have been amended, and claims 2, 12, and 22 have been canceled.

Examiner Interview

Applicants wish to thank the Examiner for the courtesy extended to Applicants' attorney during a telephone interview on April 25, 2007. During the interview, Applicants proposed amending the computer program product claims to clarify that Applicants claim a computer program product stored on a computer operable medium. The computer operable medium contains instructions for execution by a computer, which, when executed by the computer, cause the computer to implement the claimed method. The Examiner agreed that these amendments would overcome the rejections under 35 U.S.C. § 101, however, the Examiner requested that Applicants include the term "computer operable medium" in the appropriate location within Applicants' specification. Applicants have made such amendments to the claims and specification in the Response.

Applicants' attorney and the Examiner also discussed Applicants' independent claims with regard to the cited prior art. Applicants' attorney noted that the cited prior art does not disclose using encryption keys to encrypt data where the encryption keys themselves are also encrypted, as taught and claimed by Applicants. Applicants' attorney further noted that Applicants teach and claim that each user has access to a subset of the encryption keys and that each users' encryption keys are encrypted with an encryption key that is specific to the corresponding user. No agreement was reached regarding the claims during the interview.

Drawings

Applicants note with appreciation the Examiner's acceptance of Applicants' formal drawings, filed with the Application on November 21, 2003.

Amendments to the Specification

The specification has been amended to correct an inadvertent typographical error. The specification has further been amended, as requested by the Examiner during the telephone interview, to include the term "computer operable medium." No new matter has been added as a result of these amendments to the specification.

Claim Rejections Under 35 U.S.C. § 101

Claims 21-30 stand rejected under 35 U.S.C. § 101 as being directed to non-statutory subject matter. Applicants have amended independent claim 21 to clarify that Applicants claim a computer program product stored on a computer operable medium. The computer operable medium contains instructions for execution by a computer, which, when executed by the computer, cause the computer to implement the claimed method. Claim 22 has been canceled. Claims 23, 24, and 26 have been amended to be consistent with independent claim 21. Support for the amendments is found, for example, in Applicants' specification on page 21, lines 13-30. No new matter has been added as a result of the amendments.

Claim Rejections – Alleged Obviousness Under 35 U.S.C. § 103

Claims 1-30 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Kern et al., U.S. Patent No. 6,336,187 (hereinafter Kern) in view of Kohara et al., U.S. Patent Publication No. 2003/0182566 (hereinafter Kohara). Applicants respectfully traverse the rejections under 35 U.S.C. § 103.

Independent claims 1, 11, and 21 have been amended to clarify that the first subset of encryption keys includes a plurality of the encryption keys, and that a second subset of the encryption keys includes a plurality of the encryption keys. Support for this amendment is found, for example, in Applicants' specification on page 11, lines 8-13. Independent claim 1 has also been amended to include elements previously found in dependent claim 2, and therefore dependent claim 2 has been canceled. Similarly, independent claims 11 and 21 have been amended to include limitation previously found in dependent claims 12 and 22, respectively, and dependent claims 12 and 22 have been canceled.

To establish prima facie obviousness of a claimed invention, all the claim limitations must be taught or suggested by the prior art. In re Royka, 490 F.2d 981, 180 USPQ 580 (CCPA 1974). "All words in a claim must be considered in judging the patentability of that claim against the prior art." In re Wilson, 424 F.2d 1382, 1385, 165 USPQ 494, 496 (CCPA 1970). If an independent claim is nonobvious under 35 U.S.C. 103, then any claim depending therefrom is nonobvious. In re Fine, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988). (Manual of Patent Examining Procedure, § 2143.03).

Applicants respectfully submit that none of the prior art, either alone or in combination, teaches or suggests all the elements of Applicants' independent claims. Using independent claim 1 as an exemplary claim, Applicants teach and claim the following:

- encrypting a plurality of non-volatile storage regions, each being encrypted using a different encryption key from a set of encryption keys;
- making a first subset of the encryption keys available to a first user thereby granting the first user access to a corresponding first subset of non-volatile storage regions, the first subset of the encryption keys including a plurality of the encryption keys;
- making a second subset of the encryption keys available to a second user thereby granting the second user access to a corresponding second subset of non-volatile storage regions, the second subset of the encryption keys including a plurality of the encryption keys;
- generating a first private-public encryption key pair and a second private-public encryption key pair;
- making the first private key available only to the first user and the second private key available only to the second user; and
- encrypting the first subset of the encryption keys using the first public encryption key, and the second subset of the encryption keys using the second public encryption key.

Applicants teach and claim a plurality of non-volatile storage regions, where each region is encrypted using a different encryption key from a set of encryption keys. Then, a first subset of the encryption keys is made available to a first user, so that the first user has "access to a corresponding first subset of non-volatile storage regions." Similarly, a second subset of the encryption keys is made available to a second user, so that the second user has "access to a corresponding second subset of non-volatile storage regions." Kern purports to teach a storage facility that "selectively provides data-dependent security" (see Kern, Abstract). According to Kern, a host makes a storage access request for a particular storage region. If the storage region is access-key protected and the requestor provides a matching key, the operation is allowed (Kern, col. 2, line 64 through col. 3, line 4). If the keys do not match and the operation is not protected, then the operation is allowed (Kern, col. 3, lines 4-7). If the keys do not match and the operation is protected, the operation fails (Kern, col. 3, lines 7-9).

The Office Action notes that Kern does not disclose encrypting each region using a different encryption key from a set of encryption keys (see Office Action, page 5, lines 1-2). The Office Action further notes that Kern does not disclose making a first subset of encryption keys available to a first user, so that the first user has access to a first subset of non-volatile storage regions, and making a second subset of encryption keys available to a second user, so that the second user has access to a second subset of non-volatile storage regions (see Office Action, page 5, lines 2-5). However, the Office Action then cites Kohara as teaching these aspects of Applicants' independent claims.

Kohara purports to teach using a pseudorandom number to generate a plurality of encryption keys (Kohara, paragraph [0012]). However, the cited section of Kohara does not teach or suggest "making a first subset of the encryption keys available to a first user" and "making a second subset of the encryption keys available to a second user," as taught and claimed by Applicants. Even assuming, for the sake of argument, that Kohara does suggest making various subsets of encryption keys available to various user, neither Kern nor Kohara teaches or suggests encrypting the encryption keys in the manner taught and claimed by Applicants.

In addition to making a first subset of encryption keys available to a first user and a second subset of encryption keys available to a second user, Applicants further teach and claim that the first and second subsets of encryption keys are themselves encrypted. As claimed in the independent claims, a first private-public encryption key pair is generated, where the first private key is only made available to the first user. Similarly, a second private-public key encryption key pair is also generated, where the second private key is only made available to the second user. Then Applicants specifically claim that the first subset of encryption keys, i.e. the subset of encryption keys that is made available to the first user, is encrypted using the first public encryption key. Similarly, the second subset of encryption keys, i.e. the subset that is made available to the second user, is encrypted using the second public encryption key. Neither Kern, nor Kohara, nor a combination of the two, teaches or suggests Applicants' unique method of encrypting a subset of encryption keys, where the subset of encryption keys is assigned to a specific user, and where the encrypting of the subset of encryption keys is performed using a specific public encryption key that is part of a private-public encryption key pair that is also assigned to the specific user.

The Office Action cites Kern at col. 10, lines 27-35 as teaching this aspect of Applicants' claims (see Office Action, page 6, lines 8-18). However, the cited section of Kern is discussing an embodiment where "the requesting host" submits "a proper input access key to access the storage region," and then the data in the requested storage region is encoded "with the key" (Kern, col. 10, lines 32-35). Kern specifically states that the data in the storage region is encoded "with the key," i.e. with the key that has been submitted by the requesting host as the input access key. Kern is only encrypting the data in the storage region. Kern does not teach or suggest encrypting an access key which is then used to further encrypt the data in the storage region. Applicants teach and claim two levels of encryption, i.e. 1. encrypting the data in the non-volatile storage regions using the subsets of encryption keys, and then 2. further encrypting the subsets of encryption keys (using private-public key encryption as discussed above).

None of the prior art, either alone or in combination, teaches or suggests Applicants' unique method, system, and computer program product for encrypting non-

volatile storage regions with different encryption keys and then making subsets of those encryption keys available to various users. Specifically, none of the prior art, either alone or in combination, teaches or suggests that a first/second subset of the encryption keys is assigned to a first/second user and then that first/second subset of the encryption keys is encrypted using a first/second private-public key encryption pair, where the first/second private key is only available to the first/second user (to whom the first/second subset of encryption keys has been assigned).

For the reasons set forth above, Applicants respectfully submit that independent claims 1, 11, and 21, and the claims which depend from them, are patentable over Kern in view of Kohara, and respectfully request that they be allowed.

Notwithstanding the patentability of dependent claims 3, 4, 13, 14, 23, and 24 based on the above discussion, Applicants would like to further point out that these claims claim additional layers of security. For example, as claimed in dependent claims 3 and 4, the first user can only access the first private key by providing a first authentication token. If the first user provides a matching authentication token, then the first user's private key is decrypted. The first user's private key is then used to decrypt the first user's subset of encryption keys, and then those encryption keys are used to decrypt the corresponding non-volatile storage regions. This multi-layered approach to encrypting/decrypting data is simply not taught or suggested by either Kern or Kohara. While the Office Action cites numerous section of Kern to reject claims 3 and 4 (see Office Action, pages 6 and 7), the cited sections merely discuss Kern's use of a single access key, along with an operation type, in order to determine if a user may access a storage region. As discussed above, according to Kern, a host makes a storage access request for a particular storage region. If the storage region is access-key protected and the requestor provides a matching key, the operation is allowed (Kern, col. 2, line 64 through col. 3, line 4). If the keys do not match and the operation is not protected, then the operation is allowed (Kern, col. 3, lines 4-7). If the keys do not match and the operation is protected, the operation fails (Kern, col. 3, lines 7-9). Kern does not teach or suggest using an authentication token to determine if a private key should be decrypted, then using the private key to decrypt a subset of encryption keys, and then

using the encryption keys to decrypt a plurality of non-volatile storage regions, as taught and claimed by Applicants. Therefore, Applicants respectfully submit that dependent claims 3 and 4 are patentable over Kern in view of Kohara. Claims 13, 14, 23, and 24 include similar limitations to those found in claims 3 and 4, and are therefore also patentable over Kern in view of Kohara.

Conclusion

As a result of the foregoing, it is asserted by Applicants that the remaining claims in the Application are in condition for allowance, and Applicants respectfully request an early allowance of such claims.

Applicants respectfully request that the Examiner contact the Applicants' attorney listed below if the Examiner believes that such a discussion would be helpful in resolving any remaining questions or issues related to this Application.

Respectfully submitted,

By /Leslie A. Van Leeuwen, Reg. No. 42,196/

Leslie A. Van Leeuwen, Reg. No. 42,196
Van Leeuwen & Van Leeuwen
Attorneys for Applicant
Telephone: (512) 301-6738
Facsimile: (512) 301-6742